

**OCF “Ipanema+” – Clarifying when SVRS expose unsecured endpoints – Security WG
CR 3444**

Legal Disclaimer

THIS IS A DRAFT SPECIFICATION aDOCUMENT ONLY AND HAS NOT BEEN ADOPTED BY THE OPEN CONNECTIVITY FOUNDATION. THIS DRAFT DOCUMENT MAY NOT BE RELIED UPON FOR ANY PURPOSE OTHER THAN REVIEW OF THE CURRENT STATE OF THE DEVELOPMENT OF THIS DRAFT DOCUMENT. THE OPEN CONNECTIVITY FOUNDATION AND ITS MEMBERS RESERVE THE RIGHT WITHOUT NOTICE TO YOU TO CHANGE ANY OR ALL PORTIONS HEREOF, DELETE PORTIONS HEREOF, MAKE ADDITIONS HERETO, DISCARD THIS DRAFT DOCUMENT IN ITS ENTIRETY OR OTHERWISE MODIFY THIS DRAFT DOCUMENT AT ANY TIME. YOU SHOULD NOT AND MAY NOT RELY UPON THIS DRAFT DOCUMENT IN ANY WAY, INCLUDING BUT NOT LIMITED TO THE DEVELOPMENT OF ANY PRODUCTS OR SERVICES. IMPLEMENTATION OF THIS DRAFT DOCUMENT IS DONE AT YOUR OWN RISK AMEND AND IT IS NOT SUBJECT TO ANY LICENSING GRANTS OR COMMITMENTS UNDER THE OPEN CONNECTIVITY FOUNDATION INTELLECTUAL PROPERTY RIGHTS POLICY OR OTHERWISE. IN CONSIDERATION OF THE OPEN CONNECTIVITY FOUNDATION GRANTING YOU ACCESS TO THIS DRAFT DOCUMENT, YOU DO HEREBY WAIVE ANY AND ALL CLAIMS ASSOCIATED HEREWITH INCLUDING BUT NOT LIMITED TO THOSE CLAIMS DISCUSSED BELOW, AS WELL AS CLAIMS OF DETRIMENTAL RELIANCE.

The OCF logo is a trademark of Open Connectivity Foundation, Inc. in the United States or other countries. *Other names and brands may be claimed as the property of others.

Copyright © 2020 Open Connectivity Foundation, Inc. All rights reserved.

Copying or other form of reproduction and/or distribution of these works are strictly prohibited.

***** **Changes to clause 8.3** *****

<Editor's note: No changes prior to this text in clause 8.3>

- If there is no open Device Onboarding Connection, then
 - The Device shall expose an unsecured OCF Endpoint for the Resources "/oic/sec/doxm" and "/oic/sec/pstat".
 - For all SVRs other than "/oic/sec/doxm" and "/oic/sec/pstat":
 - The SVR shall not expose an Unsecured OCF Endpoint.
 - Anonymous Retrieve and Updates requests (those arriving over unauthenticated channel such as CoAP) for the "/oic/sec/doxm" Resource shall be granted.

<Editor's note: some text skipped>

- If there is an open DOC, then
 - For all SVRs:
 - The Device shall not expose an Unsecured OCF Endpoint for the SVR.
 - All requests received over the DOC which target DCRs shall be granted, regardless of the configuration of the ACEs in the "/oic/sec/acl2" Resource.

<Editor's note: No changes after this text in clause 8.3>

***** **End of Change** *****

***** **Append to each of clauses 8.4, 8.5, 8.6** *****

- For all SVRs:
 - The SVR shall not expose an Unsecured OCF Endpoint.
 - The Device shall ignore all ACEs with "subject" matching either {"conntype": "anon-clear"} or {"conntype": "auth-crypt"} when making access decisions for requests to the SVR.

***** **End of Change** *****